Defense Intelligence Agency

Department of Defense
Intelligence Management System

Accreditation Test Plan

Prepared for
DoDIMS PMO
National Intelligence Production Center
DIA/PO-5C

Prepared by
J.G. Van Dyke & Associates, Inc.
6550 Rock Spring Drive, Suite 360
Bethesda, Maryland 20817

November 14, 1994

FOREWARD

The Department of Defense Intelligence Management System (DoDIMS) Security Test Plan is being written as part of a generic set of accreditation documentation to support accreditation of DoDIMS at specific user sites. Each site will need to review this documentation and modify it, as necessary, to address specific site environment in which DoDIMS will operate.

Table of Contents

Section **Page**

Section **Page**

Section **Page**

1.0 **General**

Accreditation is the formal declaration by an accrediting authority that an automated information system (AIS) or network is approved to operate (1) in a particular security mode, (2) with a minimum prescribed set of technical and nontechnical security safeguards, (3) against a defined threat, (4) in a properly secured area in a given operational environment, (5) under a stated operational concept, (6) with stated interconnections to other AISs or networks, and (7) at an acceptable level of risk for which the accrediting authority has formally assumed responsibility. The modification of any of these conditions requires a review of its impact on the security of the information processed and could result in a reaccreditation of the system.

Accreditation is the official management authorization for operation of an AIS or network and is based, in part, on the field review of the degree to which a system meets a prescribed set of security requirements. This field review includes: (1) execution of the Department of Defense (DoD) Information Management System (DoDIMS) Accreditation Test Procedures, with (2) assessment of the proficiency of site operations personnel, as well as (3) inspection of the system security related documents listed in paragraph 3.2.1.1d of this document. The accreditation statement fixes security responsibility with the accrediting authority and shows that due care has been taken for security.

1.1 **Purpose of the Plan**

This Test Plan describes the planning which will be employed to demonstrate that the security requirements which have been levied on DoDIMS have been satisfied to the degree necessary to be accredited to operate at the Sensitive Compartmented Information (SCI) System High level. As such, this plan (1) Presents the Test Sets needed to demonstrate that DoDIMS implements the necessary security requirements and (2) contains specific guidelines on how the test is to be conducted.

The general method for accomplishing this is as follows:

a. Consolidate security requirements.

b. Group each security requirement into like subjects for implementation into one or more Test Sets.

c. Develop the Test Sets.

d. Expand each Test Set into detailed test procedures.

The objective of this plan is to demonstrate how each system security requirement pertaining specifically to the application will be demonstrated.

The activities outlined in this plan are those required to obtain formal security accreditation of the SCI DoDIMS in the areas of personnel, physical, communications, TEMPEST, procedural/administrative, and hardware/software security.

1.2 **References**

The following paragraphs contain a list of reference documents used to support accreditation of DoDIMS. These documents provide an additional source of information concerning various aspects of DoDIMS and the accreditation process.

1.2.1 **System Documentation**

a. DoDIMS Security Concept of Operations (SECONOPS).

b. DoDIMS System Security Requirements (SSR).

c. DoDIMS Threat Assessment.

d. DoDIMS System Security Analysis (SSA).

e. Information System Security Officer (ISSO) appointment letter.

f. SunOS System and Network Administration Manual, Sun Microsystems, 1991.

1.2.2 **DoD Documents**

The following list contains documents which provide supportive information for the accreditation process and its requirements:

a. Defense Intelligence Agency (DIA) Manual (DIAM) 50-3, Physical Security Standards for Sensitive Compartmented Information Facilities, FOR OFFICIAL USE ONLY

b. DIAM 50-4, Security of Compartmented Computer Operations, CONFIDENTIAL, 24 June 1980

c. DoD 5200.28-STD, DoD Trusted Computer System Evaluation Criteria, unclassified, 26 December 1985

d. DIA Regulation (DIAR) 50-37, Control of Computer Output and Verification of Computer Output Classification for Compartmented Computer Operations, unclassified, 24 March 1987

e. DoD Directive C-5200.5, Communications Security (COMSEC), CONFIDENTIAL, 15 April 1971, as amended

f. MIL-HDBK-232, Military Standardization Handbook RED/BLACK Engineering--Installation Guidelines, 14 November 1972

g. DoD Directive S-5200.19, Control of Compromising Emanations, SECRET, 10 February 1968, as amended

h. DCID/16, Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks, SECRET--REL UK/CAN/AUS, 19 July 1988

i. DoD C-5030.58-M, Defense Special Security Communications System (DSSCS)Security Criteria and Telecommunications Guidance, CONFIDENTIAL, July 1978

j. DOI-103, DSSCS Operating Instructions, System/Data Procedures, CONFIDENTIAL, January 1983

k. NACSIM 5100, Compromising Emanations Laboratory Test Standard for Electromagnetics, unclassified

l. DoD Directive 5200.28, Security Requirements for Automated Information Systems , unclassified, 21 Mar 1990

m. DIAM 50-XX, DIA Security Handbook for Automated Information Systems and Separately Accredited Networks (Draft), SECRET, 14 Dec 1990

2.0 **System Security**

2.1 **General System Description**

2.1.1 **Background**

DoDIMS is designed to support the intelligence production management requirements of the DoD and National Intelligence Community (NIC). It was developed to provide the automated tools for registering and validating production requirments (PR), deconflicting, and assigning production. It was also designed to track and manage overall production management activity.

2.1.2 **System Functionality**

DoDIMS performs 3 basic functions: 1) register Production Requests and Intelligence Products initialization/updates; 2) replicate data to DoDIMS sites; and 3) update the peer databases and Central Database.

2.1.3 **System Architecture**

DoDIMS is a client-server application developed in accordance with DoD and DIA information system architectural standards. It consists of five client modules which reside on a JDISS workstation and a database co-hosted on the workstation. Eventually a master, read-only database will be established on a dedicated server at the DIAC.

2.1.3.1 **Hardware**

DoDIMS currently utilizes a JDISS workstation to host both client application modules and a server database. All systems will be based on a standard JDISS configuration. The hardware for the master database to be installed at the DIAC is to be determined. The standard configuration is as follows, however, *site specific configurations may differ*:

- Sun SPARCStation 2/10/20 with 32 or 64 MB RAM
- Sun High Resolution Color Monitor
- Sun CD-ROM Drive
- 1.3 GB internal or 2.1 GB external hard drives (minimum)
- Ethernet Transceiver
- Two (2) serial ports
- Bi-directional Printer Port
- 8mm Tape Drive
- Mouse
- NeWSprinter CL+ Color Printer

2.1.3.2 **Software**

DoDIMS/JDISS software consists of both commercial-off-the-shelf software, DoDIMS- unique software developed under Government contract and Government-Furnished software

2.1.3.2.1 **COTS Software**

COTS software consists of the following

- SUN OS 4.1.3
- X-windows X11.R5
- OSF Motif 1.2
- Looking Glass Professional 3.0
- ApplixWare 2.1
- ELT/2 2.2.10-R4 with TACO2
- Open Connect TN3270 with graphic option
- TEEMX
- XNVDET
- Sybase 10.0.1
- Sybase Replication Server 10.0.1
- Gain Momentum Runtime
- Newsprint

2.1.3.2.2 **DoDIMS-Unique Software**

2.1.3.2.2.1 **Client Software**

DoDIMS-unique client software is in the application written in Gain Extension Language (GEL) to provide the following modules:

a. Requirements Module. This module provides the user with an automated Production Requirements (PR) process in support of both crisis and non-crisis requests. It provides the intelligence consumer a mechanism to register production requirements and forward them to the appropriate validating organization and, where applicable, any additional authorities. Once validation occurs, a production center is notified of the PRs existence. After reviewing the PR, and coordinating with collaborative production centers if appropriate, the production center sends the consumer a response on the proposed production actions. At any given time, a customer and/or validator has the ability to track the status of the PR through its organization and to the producing organization.

b. Assignment Module. As production requirements are fully validated, this module will automatically enter the responsible production center information for assignment based on geographical and functional areas. For requests comprising more than one responsible producer areas, the validator will select primary and collaborative producers. This final validating authority is empowered to override the assignment criteria as necessary. DoDIMS will not assign production without an appropriate link to a validated requirement to ensure production resources are being utilized to satisfy consumer requirements.

c. Production Module. This module makes available to the community an on-line production schedule. Production center production managers will have the ability to input and maintain their annual scheduled production. In addition, deconfliction will be accomplished as new information is submitted. An individual entering data will review perceived duplicate entries prior to submitting a new request, or initiating a new intelligence product. As products are published and production schedule records closed-out, cross-reference information will be available to assist the user in retrieving the publication through DoDIIS Dissemination.

d. Reports Module. This module makes available to its users a capability to obtain production management information by utilizing either various pre-defined or user-defined reports. Whatever the type of report, a graphics capability is available consisting of Pie, Bar, Area, line column, 3-D types of charts.

e. Assessment Module. This module provides a mechanism by which primarily production managers and functional managers obtain information regarding resource utilization, producer assessments, and production shortfalls.

2.1.3.2.2.2 **Server Software**

DoDIMS server software consists of data tables developed within Sybase, and the Replication server application.

2.1.3.2.2.3 **Government Furnished Software**

JINTACCS Automated Message Processing Software (JAMPS)

2.1.3.2.3 **Firmware**

There is no DoDIMS-unique firmware.

2.1.4 **Communications**

DoDIMS will use data networking and communications associated with the JDISS workstation. In most cases, the workstation will be attached to a dedicated LAN which will connect to JWICS or connect to a site LAN which will connect to JWICS.

2.2 **System Security Requirements**

The system security requirements for DoDIMS have been defined in the DoDIMS SSR document. A Security Requirements Compliance Matrix (SRCM) has been developed from these requirements to ensure that all security requirements are tested. The SRCM has been used as a base and a guideline from which the system accreditation Test Sets were developed and the accreditation test procedures will follow. The SRCM for DoDIMS is at appendix A to this document.

2.3 **System Test Sets**

To insure that all security requirements have been implemented in the system, "Test Sets" are developed. A Test Set identifies a group of tests to be developed in the system accreditation test procedures. A Test Set is designed to confirm the presence of one or more of the security requirements of the system. Each technical security requirement is allocated to one or more Test Sets. In this way the successful execution of the tests provides necessary evidence that the system's technical security requirements are implemented in the system.

The intent of the Test Sets is to provide a guide and point of departure for the preparation of the Accreditation Test Procedures for DoDIMS. The Test Sets provide a high level description of the tests to be developed and executed during the system's accreditation. For tracking purposes, the Test Set numbers have been correlated to the requirement numbers (e.g., the Test Set for system requirement number 25.c, "Identification and Authentication," is also numbered 25.c). In some cases a Test Set is divided into two or more sub-topics to ensure that all related requirements are included and tested; these sub-topics are identified by a decimal number following the base Test Set identification (e.g., 25.c.1).

2.3.1 **Administrative Security Test Sets**

This section addresses the test sets required to verify DoDIMS's adherence to a variety of administrative security standards. Adherence to these standards and regulations is very important for DoDIMS, as substantial security is provided by strict adherence to administrative and procedural controls for systems being accredited in the System High mode. Note that some of the following test sets do not identify system tests per se, but rather verify that specific procedural and administrative controls are in place.

2.3.1.1 **Conceptual Design, Selection of Mode of Operation, and Identification of Accrediting Authority**

Test Set 1, consisting of three sub-tests, is designed to show DoDIMS compliance with the requirements to develop the system using a systems engineering approach, identify the mode of operation, and identify the Designated Accrediting Authority (DAA).

1.a DoDIMS was developed using a systems engineering approach.

1.b The system operating mode is System High.

1.c DIA/SY-1D is the appropriate DAA.

2.3.1.2 **System Security Plan**

Test Set 2 is designed to demonstrate DoDIMS's compliance with the requirement for a System Security Plan in accordance with DCID 1/16, page III-3, item 16.

2.3.1.3 **Appointment of an ISSO**

Test Set 3 will verify the appointment of an ISSO for DoDIMS System.

2.3.1.4 **Access by Foreign Nationals**

Test Set 4 will verify procedures are in place to prevent foreign nationals from accessing DoDIMS.

2.3.1.5 **Accreditation/Reaccreditation**

Test Set 5 will verify the necessary documentation is in place showing accreditation/ reaccreditation.

2.3.1.6 **Joint Accreditation**

Not Applicable.

2.3.1.7 **Interim Approval to Operate**

Test Set 7 will verify the site possesses the necessary documentation granting approval to operate DoDIMS.

2.3.1.8 **Security Briefings**

Test Set 8 will verify that procedures are in place to document that site personnel received required security briefings.

2.3.1.9 **Automated Guard Processors**

Not Applicable.

2.3.1.10 **Protection of High Density/Transportable Storage Devices**

Test Set 10 will verify and validate procedures to protect high density transportable media and storage devices used by DoDIMS

2.3.1.11 **Memory Remanence**

Test Set 11 is designed to verify compliance of DoDIMS with the requirements to control, destroy, and properly release magnetic storage media.

2.3.1.12 **Protected Software and Hardware**

Test Set 12 is designed to test DoDIMS compliance with the requirements to protect all system hardware, software, and firmware from unauthorized disclosure, destruction, or modification.

2.3.1.13 **Shipment of Equipment to High Risk Areas**

Not Applicable

2.3.1.14 **Marking Storage Media**

Test Set 14 will verify DoDIMS compliance with the requirements to mark all removable media with external labels identifying the proper sensitivity and handling restrictions.

2.3.1.15 **Marking Printed Output**

Test Set 15 is designed to verify compliance with the following requirements for marking of DoDIMS printed output:

15.a Mark the beginning page (i.e., security banner page) with a human readable label of the system's accredited security parameter (ASP), and include appropriate warning message concerning classification and control of the output.
15.b Mark individual pages to reflect the appropriate classification, controls, and handling restrictions.

2.3.1.16 **Manual Review of Human Readable Output**

Test Set 16 will test DoDIMS compliance with requirements to provide reliable human review of output from a system with untrusted markings or labels.

2.3.1.17 **System Disposal Plan**

Test Set 17 will verify DoDIMS compliance with requirements to develop and maintain a system disposal plan.

2.3.2 **Environmental Security Test Sets**

This section addresses the test sets required to verify DoDIMS adherence to a variety of environmental security standards. Adherence to these standards and regulations is very important for DoDIMS, as substantial security is provided by strict adherence to environmental controls for systems being accredited in the System High mode. Note that some of the following test sets do not identify system tests per se, but rather verify that specific environmental controls are in place.

2.3.2.1 **COMSEC**

Test Set 18 is designed to verify DoDIMS compliance with all applicable COMSEC regulations and local policies for systems handling Top Secret SCI material.

2.3.2.2 **Use of Dial-up Lines**

Not Applicable.

2.3.2.3 **TEMPEST**

Test Set 20 will verify DoDIMS compliance with the national policies and local Defense Intelligence Analysis Center (DIAC) regulations on compromising emanations.

2.3.2.4 **Physical Security**

Test Set 21 is designed to verify that the physical security afforded all DoDIMS components is commensurate with the processing of SCI in accordance with the provisions of DIAM 50-3.

2.3.2.5 **Personnel Security**

Test Set 22 will verify that all DoDIMS users are cleared, approved for access, and have appropriate need to know approvals for all data processed by or stored within the system.

2.3.2.6 **Commercial Vendor Maintenance**

Test Set 23 is designed to verify DoDIMS compliance with regulations requiring specific controls for system access by commercial maintenance personnel to include procedures for proper escorting of uncleared maintenance personnel.

2.3.3 **Technical Security Test Sets**

These test sets are designed to test DoDIMS compliance with the technical system security requirements for accreditation in the System High mode of operation. These requirements are contained in DCID 1/16, DIAM 50-4, and DoD 5200.28-STD (the "Orange Book"). For System High mode DoDIMS must therefore meet the requirements for "Controlled Access Protection, or Level C2, as defined in the Orange Book in order to be successfully accredited. The technical test sets that follow form the basis for most of the actual system security accreditation test procedures for DoDIMS. While these test sets offer a high level description of the functionality to be tested, the test procedures themselves describe the exact procedures to be followed and the expected results from each step. The test sets below are in some cases broken down into multiple subsets which may be further decomposed into multiple procedures in the test procedures document in order to test DoDIMS with sufficient detail to permit the Test Director and the Accrediting Authority to accredit DoDIMS to operate in the System High mode.

2.3.3.1 **Discretionary Access Control**

Test Set 25.a is designed to test DoDIMS discretionary, or need to know, access control mechanisms required to protect records in DoDIMS. This test set is divided into the following sub-topics:

25.a.1 Discretionary Record Access. Verify that DoDIMS protects access to the operating system, other system files (to include audit data), user files, group files, etc., with read/write privileges to the granularity of the individual user.

25.a.2 Discretionary Application Access. Verify that DoDIMS protects access to application and other programs with read/write/execute privileges to the granularity of the individual user.

25.a.3 Access Control Integrity. Verify that access control lists can be modified only by a process that owns the object or by a process that is privileged to override discretionary access checking.

2.3.3.2 **Object Reuse**

Test Set 25.b is designed to test DoDIMS's ability to ensure that when an object is initially assigned, allocated, or reallocated to a subject from the system's pool of unused memory objects, the object has been cleared to ensure it contains no data for which the subject is not authorized. This test set is also designed to test DoDIMS's ability to clear memory objects allocated for use by a process at run time prior to the process initially reading it.

2.3.3.3 **Identification and Authentication**

Test Set 25.c is designed to test DoDIMS's identification and authentication mechanisms. This test set is divided into the following sub-topics:

25.c.1 User Identification Authentication. Verify that all user are required to identify themselves and provide an authentication mechanism prior to being allowed to access the system.

25.c.2 User Functionality. Verify that each individual user id identified by DoDIMS is limited to proper commands, menu options, and system functions for which the user has been granted and what capabilities the user has.

25.c.3 ISSO Functions. Validate the ISSO functions, including creation of new user/user id's/passwords, and the system's ability to allow or deny access to the system. Verify that the system locks out a user after three invalid attempts to log in and that the ISSO can re-enable user IDs after lockouts occur.

25.c.4 Password Integrity. Test the integrity of DoDIMS passwords by verifying that unauthorized users cannot access system password data.

2.3.3.4 **Audit**

Test Set 25.d is designed to test DoDIMS ability to effectively create, maintain, and protect from unauthorized access or destruction an audit trail of security related system activity as defined in the requirements documents for the audit function. Specifically, this test set is designed to test DoDIMS System audit capabilities not tested as part of other test sets and to verify the associated data reduction and formatting tools. This test set is divided into the following sub-topics:

25.d.1 Audit of Logon/Logoff. Verify that the DoDIMS System audits each individual user logon and logoff. Verify that the audit record for each event includes the user identification (ID), terminal ID, date and time, and success or failure of the action. Verify that both system startup and user logon audit records include the password entered, if the action failed.

25.d.2 Audit of Discretionary Access Control. Verify that DoDIMS audits the execution, start, and cease of DoDIMS processes, object open/execute/close, object creation/deletion/modification/renaming, and changing of discretionary access controls by either a user (including the ISSO) or a process. Verify that the audit records, as appropriate for the action, include the user id, terminal ID, process ID, Object ID, object's security level, type of event (i.e., read, write, execute), date and time, and success or failure of the action.

25.d.3 Audit of Use of Privilege and Authorization. Verify that DoDIMS audits the use or attempted use of privilege or authorization (e.g., attempts to use "root" accounts; creation or modification of users, IDS, passwords, or privileges) by any system user; this includes the ISSO and system operations and maintenance personnel.

25.d.4 Audit File Protection. Verify that DoDIMS protects the audit file from modification, unauthorized access, and destruction. Also verify that users authorized to review the audit data have read only access to the audit file.

25.d.5 Audit File Maintenance. Verify that DoDIMS generates an alarm when the regulated audit space is approaching maximum capacity, that the current audit data file can be successfully transitioned to an archive audit data file, that the audit data files cannot be automatically deleted from disk, that an archive audit data file may be restored to disk for review, and that the audit file is maintained in a machine readable and searchable form (whether on-line or archive) for a period of one (1) year.

25.d.6 Audit File Review. Verify that DoDIMS allows the ISSO or other authorized personnel to access the audit trail data (both on-line and archive) for security review. Verify that the reviewer has the ability to selectively audit actions of any one or more users based on individual identity and/or of any file or program security level. Verify that the audit trail data or any selected subset can be printed at the request of the ISSO or other authorized personnel.

2.3.3.5 **System Architecture**

Test Set 25.e is designed to test DoDIMS's ability to isolate the resources it protects from access from other than an authorized individual and/or terminal. Additionally, this test set will also test the system's ability to limit system access only to authorized individuals and/or terminals.

2.3.3.6 **System Integrity**

Test Set 25.f is designed to test the ability of DoDIMS to perform self-diagnostics each time it is started to validate the correct operation of the hardware and firmware elements of the system. This self test will be evaluated to ensure that it assures that a correct copy of the operating system and applications software is booted during system startup. The test will also test the ability of DoDIMS to isolate the resources it protects from other than an authorized individual and/or terminal. It will also test the system's ability to limit system access only to authorized individuals and/or terminals.

2.3.3.7 **Security Testing**

Test Set 25.g includes the totality of all DoDIMS security testing, and, therefore, no specific test procedures will be developed for this test set. The requirements for security testing are completely met by completion of all the procedures in the Accreditation Test Procedures for DoDIMS, which are derived directly from the test sets definition in this document. Any flaws discovered during the testing process will be corrected and retested.

2.3.3.8 **Security Features User's Guide**

Test Set 25.h will identify the appropriate documents and the applicable sections in each that instruct users in the security features of DoDIMS.

2.3.3.9 **Trusted Facility Manual**

Test Set 25.i will identify the appropriate documents and the applicable sections in each to meet this requirement to document how privileged users such as the ISSO and System Administrator control the security features of DoDIMS and maintain and examine the audit file.

2.3.3.10 **Test Documentation**

Test Set 25.j will consist of an examination of the DoDIMS Accreditation Plan, Accreditation Test Procedures and the Accreditation Test report for adequacy.

2.3.3.11 **Design Document**

Test Set 25.k will consist of an examination of DoDIMS design documentation for and explanation of and adequacy of the design and implementation of security functions.

2.3.3.12 **Identification of User Terminals**

Test Set 25.l is designed to test the ability of DoDIMS to positively identify a workstation attempting to access data or applications resident on the server or its connected peripheral data storage devices prior to granting the requested access. The process of identifying the terminal will be verified as occurring prior to, or concurrent with, that of authorization checking to ensure the user or process requesting such access is properly authorized.

2.3.3.13 **Configuration Management**

Test Set 25.m is designed to demonstrate DoDIMS compliance with requirements for a configuration management system. The configuration management system used by DoDIMS will be verified as recording all changes to any line of source or object code for DoDIMS software (including commercial products), who made the change, for what reason, and when the change was made.

2.3.3.14 **Trusted Distribution**

Test Set 25.n will consist of an examination of project management office (PMO) and site procedures that provide for trusted distribution of DoDIMS software.

3.0 **Test Sequence**

3.1 **Pre-Test Activity**

The following paragraphs identify activities required to be accomplished prior to the actual accreditation test.

3.1.1 **Prerequisites of System Accreditation**

Approximately 60-90 days prior to scheduled accreditation, the DAA will provide Site Test Coordinator with a pre-accreditation letter with enclosures containing the following:

a. Statement of Content for an ADP Security Accreditation Test Report

b. A set of mailing addresses necessary for coordination and staffing of the final Test Report.

The user organization (Site Test Coordinator) and/or Executive Agent (DIA/PO-5C) is responsible for completing the report, adding and/or modifying the information provided to reflect the specifics of DoDIMS. The Test Report (with the exception of Test Findings, Recommendations, and Conclusion sections) must be completed by the user organization and/or Executive Agent prior to test team arrival.

Prior to accreditation the user organization and/or Executive Agent must complete a series of additional requirements, to include compliance with appropriate personnel, physical, communications, and TEMPEST security regulations.

Various coordination must take place between the participating agencies and the test site prior to arrival of the test team. This coordination may include, but may not be limited to, items such as provision of fund cites, billeting arrangements, etc. These requirements are the responsibility of the test coordinator and are outlined in the Test Coordinator section of paragraph 3.2.1.2 of this document.

3.1.2 **Accreditation Pre-test**

Prior to the accreditation, a complete "dry run" of the accreditation test will be performed. This test will be conducted by the Test Site Coordinator a minimum of three work days prior to scheduled accreditation. The pre-accreditation test will be conducted on the system to be accredited, using all test procedures approved by the DAA (i.e., DIA/SY-1D) for the actual accreditation test. Additional tests may be added as desired. DIA/SY-1D will also conduct appropriate security inspection of documentation and will look at compliance with physical and personnel security requirements.

This pre-test dry run will be conducted as though it is the actual accreditation test, and the pre-accreditation Test Director will maintain a test log containing a complete chronological record of tests conducted, problems encountered, corrective action taken, and other significant events. This log will be provided to the accreditation Test Director at the beginning of the actual accreditation test.

3.2 **Test Activity**

The following paragraphs identify responsibilities of the test team members and the activities they will perform in support of the accreditation test.

3.2.1 **Test Team and Responsibilities**

The Test Team will include, as a minimum, representatives from the DAA (DIA/SY-1D) or its authorized delegated agency, the user organization, and the Executive Agent/developer (DIA/PO-5C). The JDISS PMO will appoint a Test Coordinator, test operators, and test support personnel. The name of each Test Team member will be recorded in the System Accreditation Test Report.

3.2.1.1 **Test Director**

The Test Director is appointed by the DAA (DIA/SY-1D) and as such is his direct representative, responsible for ensuring that the DAA's policies are enforced under the test and by the test team. All modifications of or deviations from approved test procedures must be approved by the Test Director. Test Team members and test support personnel will be briefed by the Test Director as to their duties, the test objectives, test schedules, etc., prior to the start of testing. During actual testing the following guidelines will apply, and the Test Director will:

a. Validate that fully qualified operators are provided by the local operating unit.

b. Validate that only test records approved and authenticated by the Test Director will be used during testing.

c. Validate that the results of each test step are correct and properly documented prior to performance of the next step.

d. In the event of an equipment malfunction, software problem, or any other discrepancy, the Test Director, in coordination with the test team members, will determine if the test should proceed or halt until the problem is corrected. In the event the testing is allowed to proceed, any portion of the test that is bypassed will be retested. For hardware problems, the system maintenance personnel will be consulted.

e. Verify that a Test Log is maintained per directions provided in paragraph 3.2.1.7 of this document.

3.2.1.2 **Test Coordinator**

The Test Coordinator is designated by the user organization and/or Executive Agent (DIA/PO-5C) and is responsible for but not limited to the following:

a. Organizing the test Team

b. Serving as site point of contact for all administrative support of the Accreditation Test Team and the Pre-accreditation Test Team

c. Preparing the Security Accreditation Test Report

d. Ensuring that all documents required at accreditation time are made available for the Test Team. These documents will include the following:

(1) Certification Statements, <u>signed</u> by authorized persons:

(a) Physical security

(b) TEMPEST security

(c) COMSEC

(d) Personnel security, both users and maintenance personnel

(e) Network connections

(f) System (Note: DCID 1/16 states that "an independent team of security officials" should test the security features of the system and, on the basis of this test, "certify to the accrediting authority the degree to which the system has implemented both technical and nontechnical security measures.")

(g) Existing AIS/network accreditation (if applicable)

(2) System Security Accreditation Test Report (Note: The pre-test portion of this report is to be created by the system user and/or Executive Agent and submitted to the accreditor prior to the formal accreditation test.)

(3) Security regulations and special procedures

(a) Service/Agency/Command/Unit regulations (as applicable)

(b) Appointment document for ISSO

(c) Standard Operating Procedures for ISSO, operators, and users (e.g., ISSO's Position Handbook, System Users Guide)

(d) Memoranda of Understanding (MOUs)/Memoranda of Agreement (MOAs) for interconnection with other systems (if applicable)

(e) Configuration Management Plan and Procedures

(f) Maintenance procedures/agreements/provisions

(g) Escorting procedures

(h) Media Sanitization, Declassification, and Release Procedures

(i) Security Incident Reporting Procedures

(j) Contingency Plans (including Emergency Destruction Procedures)

(k) DIAM 50-4

(l) DoD C-5030.58-M (if applicable)

(m) Defense Information Systems Agency (DISA) Circular 370-D195-3 (if applicable)

(n) Security Test Plan and Procedures (unless test team has stated they will bring their own copies) (Note: Advance copies should be provided to DIA/SY-1D, DISA (if applicable), and the DAA at least 30 days prior to the scheduled accreditation test.)

(o) Communication Concept of Operation (unless test team has stated they will bring their own copies) (Note: Advance copies should be provided to DIA/SY-1D, DISA (if applicable), and the DAA at least 30 days prior to the scheduled accreditation test.)

e. Scheduling all meetings, briefings, or courtesy visits deemed necessary by the Test Director

f. Scheduling all external communications requirements in advance, and verifying at least 24 hours prior to scheduled accreditation test. A final confirmation should again take place approximately 30 minutes prior to scheduled time of use.

g. Ensuring that test facilities are prepared and ready to support the test and that all support personnel are present

h. Ensuring that hardware is operational and the system is properly configured before the test is allowed to begin.

i. Conferring with the Test Director to resolve anomalies.

3.2.1.3 **Test Team**

The Test Team is composed of (1) evaluators, (2) equipment operators, and (3) support personnel provided by the site. During conduct of the test, these personnel work for the Test Director, should be assembled prior to his arrival, and will remain in force until released by the Test Director. The Test Team will be readily available during scheduled test periods and will be responsible for but not limited to the following:

a. Be familiar with the location of operational and security related documents, and know how to use them.

b. Be familiar with and practice compliance to DoD, DIA, and DIAC security regulations and policies.

c. Know who the system security officers (ISSOs, etc.) are and be aware of procedures for contacting them any time, day or night, should the need arise.

d. Ensure that all classified material generated during testing is collected, properly marked, and safeguarded, as applicable

e. Ensure that all hardcopy test results generated during testing are retained until analyzed and released by the Test Director

3.2.1.4 **Test Environment**

Prior to testing, DIA/PO-5C and the Site Test Coordinator must properly configure the system for testing. The accreditation test must be conducted on the intended operational system hardware and software. Any deviation from this must first be approved by the Test Director. Coordination of all external communications and other test related coordination activity is further described in Test Coordinator Responsibilities, paragraph 3.2.1.2 of this document.

3.2.1.5 **Pre-brief**

Prior to the start of the accreditation test, the Test Director will conduct a briefing to appropriate site personnel. Attendees should include the Test Team and support personnel, as well as other interested personnel designated by the site. During the brief the Test Director will define the goal of the accreditation Test Team and explain what the expected outcome will be based on satisfactory or unsatisfactory testing and inspection results.

3.2.1.6 **Test Execution**

The Accreditation Test Procedures for DoDIMS will contain step-by-step instructions and thus provide the means by which the Test Director is assured that all security requirements are tested. The test is conducted under direct control of the Test Director at all times, and the Test Director is responsible to ensure that all tests are performed correctly and that the expected results are obtained. A detailed check of all test results must be performed, and nothing is "assumed." This check is normally a visual inspection and is accomplished by comparing test output(s) to the expected results identified in the test procedure. The result of this comparison determines success or failure of that particular test. Before a test is declared a failure based upon unexpected results, the Test Director must ensure that the error is not document related. If the observed output is identical to the expected result (other than expected specified exceptions such as date and/or time), then the test is determined to be successful and the step being executed is so marked in the Test Log and in the test procedure document, if required. Any result other than the "expected" must be analyzed to determine whether a failure has occurred or whether the expected result identified in the test procedure is in error. If the latter occurs, the proper annotations must be made in the Test Procedure document. If the test step has been determined to be a failure, further analysis must be performed to determine if retesting can be done immediately without interfering with future test steps, or if it is necessary to backup to retest, to determine if it is more efficient to perform this retest now or return to it at a later time. Should the failure be catastrophic in nature, the Test Director must determine the appropriate action to be taken. In all cases, the proper annotations must be made in the Test Log and/or Test Procedures document.

3.2.1.7 **Test Log**

During the accreditation test a daily Test Log will be maintained by the Test Director or a delegated representative. If the Test Procedures document provides the necessary space for recording this information on each test sheet, it may serve as the Test Log; otherwise, a separate Test Log must be generated. This log will contain at a minimum a chronological list of tests conducted, start-stop times, problems encountered, corrective action taken, and other significant events. This log is an official document and will be retained as part of the Security Accreditation Test Report.

3.2.1.8 **Data Recording, Reduction, and Analysis**

Data recording will consist of but not be limited to items such as line printer listings, disk or tape file output, or work station displays presented in human readable formats. Data reduction and analysis will be performed during test execution and during post-test activities (e.g., audit trail analysis may either be performed as tests are completed or at the conclusion of testing). It is recommended that audit trail review be conducted at specified intervals, reviewing several hours of tests, or at the conclusion of selected tests.

3.3 **Post-Test Activity**

The following paragraphs identify activities to be accomplished after the actual test procedures have been successfully accomplished.

3.3.1 **Accreditation Test Report**

The System Accreditation Test Report will be completed prior to release and departure of the Test Team. The "Findings and Requirements" section of this document may be completed as the test progresses and will contain a detailed explanation of all test results determined to be in error. Each test "finding" will result in either (1) a requirement, (2) a recommendation, (3) a comment, or (4) a combination thereof. Any member of the Test Team has the right to express his or her opinion or comment even when other members are not in agreement. In many cases the requirements can be satisfied on the spot, or at least prior to departure of the Test Team. If this occurs, the Test Report will reflect that the requirement has been satisfied. Requirements not satisfied prior to Test Team departure will be termed as outstanding requirements and will be classed into one of three categories:

a. Must be fixed before "Interim Authority to Operate" can be granted

b. Will not prevent the Interim Authority from being granted, but must be fixed before a final accreditation approval can be granted

c. Minor problem that must be resolved but will not prevent the system from becoming operational

Also found in this section are findings that result in no requirement to the site but are provided as recommendations only. These are generally recommendations that may "streamline" or improve an operational procedure, etc.

The "Recommendations" and "Conclusion" sections will be prepared by the Test Director at the appropriate time and will be provided to the site in sufficient time to be included in the Test Report, as will the "Discussion" section, when applicable. These sections will be prepared upon completion of all inspections, test, and test analyses; will contain at a minimum a summary of all findings, requirements, and recommendations; and will indicate their status at test completion (either completed or outstanding). Based on the type and quantity of outstanding requirements, the Test Director will determine a pass or fail statement and will either:

a. Grant Interim Authority to Operate with approval to begin immediately;

b. Grant Interim Authority to Operate with approval to begin at a later date, pending satisfactory completion of certain outstanding requirements; or

c. Reject the accreditation due to serious hardware, software, or security-related problems that cannot be resolved in the near future and such that upon resolving would require a complete Security Accreditation retest.

3.3.2 **Out-brief**

After completion of all tests, analyses, and final preparation of the Accreditation Test Report, the Test Director will conduct an Out-brief, attendees of which are determined by the site. The purpose of the out-brief is to discuss the Test Report, its contents, and its purpose. The briefing will cover the "Test Findings and Requirements" and "Recommendations," discussing each one individually and focusing on outstanding requirements and their impact in respect to the system accreditation and/or the site's Interim Authority to Operate pending final accreditation approval (paragraph 3.3.4 of this document).

3.3.3 **Interim Authority to Operate**

An Interim Authority to Operate is granted by the DAA and is authorized to allow a site that has satisfactorily completed accreditation testing to begin operations pending completion of the Final Accreditation approval process. The Final Accreditation is further described in the following paragraph.

3.3.4 **Final Accreditation**

Prior to departure of the Test Director, the System Accreditation Test Report must be completed. It will be staffed for comment through the site's chain of command to the Director, DIA, requesting final accreditation approval. This staffing and approval process will vary from three to four months, during which time the site may be granted Interim Authority to Operate (see paragraph 3.3.3 of this document). This interim authority to operate is dependent upon completion of outstanding requirements as described in paragraph 3.3.2 of this document.

APPENDIX A

SECURITY REQUIREMENTS COMPLIANCE MATRIX

Security Requirement	Security Requirement Title	Test Number
1a	Conceptual Design	1a
1b	Mode of Operation	1b
1c	Identification of Accrediting Authority	1c
2	System Security Plan	2
3	Appointment of ISSO	3
4	Access by Foreign Nationals	4
5	Accreditation/Reaccreditation	5
7	Interim Approval to Operate	7
8	Security Briefings	8
10	Protection of High Density/Transportable Storage Devices	10
11	Memory Remanence	11
12	Protected Software and Hardware	12
14	Marking Storage Media	14
15	Marking Printed Output	15
16	Manual Review of Human Readable Output	16
17	System Disposal Plan	17
18	COMSEC	18

20	TEMPEST	20
21	Physical Security	21
22	Personnel Security	22
23	Commercial Vendor Maintenance	23
25.a	Discretionary Access Control	25.a
25.b	Object Reuse	25.b
25.c	Identification and Authentication	25.c
25.d	Audit	25.d
25.e	System Architecture	25.e
25.f	System Integrity	25.f
25.g	Security Testing	25.g
25.h	Security Features User's Guide	25.h
25.i	Trusted Facility Manual	25.i
25.j	Test Documentation	25.j
25.k	Design Documentation	25.k
25.l	Identification of User Terminals	25.l
25.m	Configuration Management	25.m
25.n	Trusted Distribution	25.n

APPENDIX B

TERMS AND ABBREVIATIONS

AIS	Automated Information System
ASP	Accredited Security Parameter
COMSEC	Communications Security
COTS	Commercial Off the Shelf
DAA	Designated Approving Authority
DCID	Director of Central Intelligence Directive
DIA	Defense Intelligence Agency
DIAC	Defense Intelligence Analysis Center
DIAM	Defense Intelligence Agency Manual
DIAR	Defense Intelligence Agency Regulation
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDIMS	DoD Intelligence Management System
DSSCS	Defense Special Security Communications System
GEL	Gain Environment Language
ID	Identification
ISSO	Information System Security Officer
JDISS	Joint Deployable Intelligence Support System
JWICS	Joint World-wide Intelligence Communications System
LAN	Local Area Network
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIC	National Intelligence Community
OS	Operating System
PMO	Program Management Office
SCI	Sensitive Compartmented Information
SECONOPS	Security Concept of Operations

SRCM	Security Requirements Compliance Matrix
SSA	System Security Analysis
SSR	System Security Requirements Document